Joint air operations center, Millennium Challenge.

99th Communications Squadron (Molly Gilliam)

Information Operations and Millennium Challenge

By MARK W. MAIERS and TIMOTHY L. RAHN

Millennium Challenge, a joint exercise hosted by U.S. Joint Forces Command (JFCOM) in summer 2002, examined how far the Armed Forces could go in implementing *Joint Vision 2020* and executing rapid decisive operations within this decade. One goal was to develop recommendations on doctrine, organization, training, manpower, logistics, personnel, and facilities. Exercise live play was focused on operational net assessment, identifying critical nodes, the range of options, second- and third-order effects, and unintended consequences. The services mounted live actions with combat assessments and employed effects-based operations to pursue experimentation goals.

From the outset of the exercise it was apparent that information operations could produce decisive effects in the fight. These efforts integrate military deception, psychological operations, electronic warfare, operational security, and computer network operations. They affect the enemy information environment while not affecting

Lieutenant Colonel Mark W. Maiers, USA (Ret.), was the information operations supervisor and Major Timothy L. Rahn, USAR, served in the combatant command information operations cell during Millennium Challenge.

friendly audiences. Ultimately, these operations seek to influence enemy decisions and opinions in ways favorable to national objectives.

Another goal of the exercise was integrating information operations in rapid-decisive and effects-based operations constructs to gain and maintain information superiority. The concept of operations was the initial step in the experiment and adhered to current doctrine. It involved testing the standing joint force headquarters (SJFHQ), which provided combatant commanders with a trained, equipped, and permanently constituted joint organization. This headquarters was intended to reduce lag time for setting up a JTF headquarters to conduct operations. Once the exercise began, the staff was augmented to form a cross-functional body composed of five groups: operations, plans, information superiority, information/knowledge management, and a command element, which worked without formal or informal barriers.

there was no national doctrine, strategy, or process promoting integrated information operations

Thus information operations supported the joint task force in an environment heavily reliant on information and information systems. Both were meant to increase knowledge of an enemy and to protect command and control and situational awareness. Information superiority is achieved by negating enemy capabilities until the Armed Forces dominate the information domain without effective opposition.

Most information operations staff members were part of the information superiority group. Primary duties under the original concept were synchronizing information operations, maintaining the operational net assessment, developing the effects tasking order, integrating information effects into the overall mission, assessing the effects of information operations, and identifying intended and unintended enemy reactions. The staff worked with organizations external to the joint task force to accomplish these tasks.

Growing pains appeared as the exercise progressed. It became clear that the information portion was not vigorous enough to gain and sustain information superiority. As such, operations directly reflected the situation in the defense establishment. Capabilities are not well understood by all planners and leaders. There are disparate service centric information operations capabilities, with little agreement on how they should be used together in support of joint operations. During the exercise, Joint Pub 3-13, *Information Operations*, was in the process of rewrite, with over 200 critical comments on the first review. DOD Directive 3600.1, though not yet published, was in its seventh revision. The services and U.S. Special Operations Command were responsible for tactics and doctrine, JFCOM for testing and experimentation, and U.S. Space Command for computer network defense and attack. The information operations study that Defense Planning Guidance directed was not yet complete.

Setting the Stage

As exercise planning commenced, there was a lack of overarching national policy, with no national doctrine, strategy, or process promoting integrated information operations. The interagency coordination and approval process was geared to separately established Presidential directives concerning functions such as contingency operations and critical infrastructure protection. SJFHQ and the component commands did not have enough trained and experienced personnel to conduct full spectrum information operations. Inadequate resources existed for producing effective perception management results such as integration of cultural intelligence, psychological operations (PSYOP), public affairs, and civil affairs. There was insufficient intelligence support for technical options in conducting a computer network attack and for integrating and conducting operations with coalition and allied information operations players. In addition, there was a need to ease and streamline the restrictive security accesses for existing capabilities.

The need to fix information operations is understood on the national level. Requirements and instructions for military information capabilities are clearly and consistently outlined in recent defense guidance as follows:

- Operations will be synchronized with multinational and interagency partners as required.
- Information operations may evolve into a separate mission area requiring the services to maintain appropriately designed organizations and trained specialists.
- The ability to conduct information operations has become a core DOD competency.
- It is imperative to maintain an unsurpassed capability to conduct information operations.

The Challenges

Millennium Challenge provided a test for finding solutions to the challenges of information operations. Given a near-peer competitor and the requirement to conduct rapid decisive operations in the future, how can actions be measured to determine when information operations are effective? Many believe information superiority, like air superiority, can be gained only for limited periods, so a reliable way of measuring success is needed. Comparing measures of performance and effectiveness offers a way of identifying when windows of information superiority exist.

It became obvious during the exercise that the organization was inadequate for information operations. Functional aspects were dispersed with no one commander coordinating activities, and information operations were only partially represented by the joint psychological operations task force, which is equally important to plans and information superiority. Early in the exercise the JTF commander recognized information operations as a capstone element of combat power both in the lethal and nonlethal sense.

Information operations cell. The organization combined enabling effects, guidance/intent, and the critical information requirements list in the information operations part of the effects

Launching Dragon Eye, Millennium Challenge.

U.S. Air Force (John Houghton)

tasking order. It was not envisioned as an annex or stand-alone plan, but as an integration of operations across the priority effects list that components use in developing plans in support of the order. The assessment process would be critical and should be driven by the objectives of JTF commanders and not exclusively by a list of effects.

Network analysis. Future cells must be furnished with suitable analytical products. A full network map of the communications architecture and complete analysis of the regional infrastructure should be primary tools in understanding enemy targets. Additionally, strategic influence analysis modeling of political and economic networks is needed. Only partial versions of these products were available as separate networks in the exercise, with no initial analysis on how they were interconnected. Subsequent targeting analysis by the joint force air component commander, combined air operation center, and JTF joint intelligence support center were not synchronized. The combined air operation center used the Telescope system, while the joint intelligence support center relied on the Adversary software tool. The latter performed marginally, resulting in attrition as opposed to targeting the systems that had the most bang for the buck.

Defense information operations. The exercise focused almost exclusively on the attack and exploitation capabilities of offensive information operations; little defense was played. There was minimal cyber event reporting and none in the joint operational area. Similarly, red forces made only a slight effort to dazzle and jam space assets. Future JTFs must consider the reality of the threat to networks, nodes, and transmission centers. During the exercise, asymmetric attack on friendly operations was unrealistic compared with the scope of the simulation.

few defensive information operations were built into the exercise design

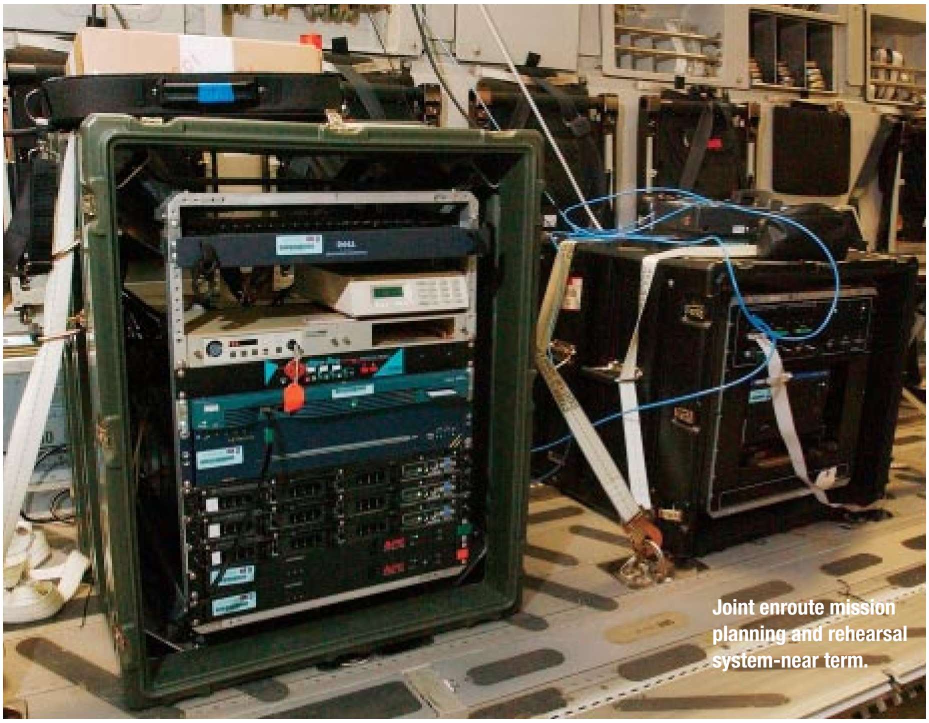
While few defensive information operations were built into the exercise design, the cell did work on defensive issues. It tracked trends in analyses of friendly networks, communication nodes, and outside influences on the joint task force.

Cyberwolf. Computer network attack activity in blue force systems and subsystems was measured using Cyberwolf. The software had the desired effect by getting organizations to change information conditions in the theater. It identified network scans and potential intrusion, but it was not the only indicator. It was adequate only when combined with information external to the serviced network. Cyberwolf was a qualified success. Injects were limited to the first phase of operations prior to H hour. They sensitized the JTF staff to a dependence on digitized information handling and highlighted the fact that a change in information conditions impacts, but is not understood by, mid and upper levels of leadership. Every component has the authority to change the conditions, normally in concert with joint task force computer network operations, which maintains a common operating picture. In Millennium Challenge, components changed conditions without consulting outside organizations or considering the global ramifications in a stressed environment.

The relevance of information conditions in this exercise, where information workspace was the primary means of JTF command and control, reveals that the entire process should be reviewed and synchronized. During the exercise, workspace used the secret Internet protocol router network (SIPRNET) without a redundant system. Disconnecting systems, as required under information condition Charlie, is not an option. Commanders will face this same problem in the future should an enemy find the means to degrade friendly databases, nodes, and transmission capabilities.

Space and Information Operations

U.S. Space Command provided a space and information operations element on the level of the combatant commander during Millennium Challenge to give enhanced support to rapid-decisive operations, effects-based operations, and operational net assessment. It contributed personnel and



Joint enroute mission planning and rehearsal system-near term.

1st Combat Camera Squadron (Lisa M. Zunzanyika)

supported the information operations cell, which must be available in every JTF operation. In the near term, information expertise should be provided to combatant commanders from the relatively small pool of expertise in DOD. However, expertise will eventually need to become resident in the commander's staff to provide full integration into both deliberate and crisis planning.

External organization support. Centers of excellence were mentioned frequently during the exercise, but their capabilities were not drawn upon. Agencies could reasonably be expected to be available over SIPRNET, but private sector resources such as educational institutions would not in a classified scenario. Furthermore, posing specific questions would violate operational security. Connectivity with agencies such as Joint Warfare Analysis Center, Joint Information Operations Center, joint task force computer network operations, 1st Information Operations Command, Fleet Information Warfare Center, Central Intelligence Agency, and Defense Intelligence Agency would have proven invaluable and should be part of future JTF operations.

Analysis tool development. Current information operations doctrine and most of the tools that supported planning involve a mechanical, stovepiped approach based on the joint operation planning execution system. Information operations do not fit that mold. Analysis of the problem of isolating unfriendly command and control yielded various methods by which an enemy obtains information and makes decisions. The information operations staff evaluated physical contacts, the electromagnetic spectrum, hard copy media, and intelligence apparatus. The associated nodes were identified, which eventually linked to the targets necessary to focus on a specific enemy capability. The team avoided stovepiping in its approach to the problem, resulting in integrated and synchronized solutions. The development of this formal approach to analysis of the information environment will be critical to future JTF operations.

Spectrum analysis and deconfliction. A requirement for a joint restrictive frequency list or spectrum manager was identified early in the exercise. A joint force air component commander had nominal responsibility as part of the real-world live fire portion. However, an analysis of the total radio frequency spectrum was needed to identify the part the enemy was using and the part JTF was using. The information operations cell conducted an initial analysis but could not gain sufficient intelligence to create a viable tool for attacking or exploiting enemy use of the radio spectrum. The ability to understand, exploit, deny, and protect across the full range of frequencies must be considered in future exercises, experiments, and real world events.

Technical Skill Sets

Manning information operations cells is a challenge. During the exercise the cell had electronic warfare specialists from the Navy and Air Force, a PSYOP officer, two computer network operations planners (a marine and an airman), but no dedicated planners for deception or operational security. In addition, there were no dedicated targeteers or intelligence support personnel. All operators were specialists in information and service-specific capabilities, but few had significant backgrounds, and all had difficulty understanding the larger concept. This problem will persist until the services further develop career patterns for planners. Key personnel and skill sets are required for SJFHQ and information operations components:

- information operations specialists who have expertise in areas such as electronic warfare and computer network operations and a general understanding of information capabilities and centers of excellence that can provide in-depth analysis for planning
- planners able to use information operations in support of the overall JTF plan, understand their capabilities and application on the national level, and develop measures of performance and execution
- special technical operations planners who understand technical operations capabilities and how they can support information operations
- intelligence analysts who specialize in intelligence but grasp the requirements for planning, executing, and assessing information operations
- system of systems analysts who are experts on the operational net assessment database and have sufficient knowledge of

information operations to support planning and analysis activities

- effects assessors who can evaluate the effectiveness of information operations both generally and in relation to the overall plan.

There are five core capabilities of information operations divided into two camps. On one side are technologists, who provide electronic warfare and computer network attack/defense to affect the electromagnetic spectrum and information systems. On the other are humanists, who conduct PSYOP, military deception, and operations security to influence foreign decisionmakers and protect friendly decisionmakers. Unifying both groups into a single core of specialists is key to understanding the capabilities that must be integrated on all levels of warfare.

A Joint Task Force

One important observation in Millennium Challenge was the requirement on the part of the blue force for a central coordinator on the JTF level. Only PSYOP was addressed formally on the command level by the joint psychological operations task force. During the exercise, information operations achieved component-level status with respect to responsibility but lacked the resources and authority to be genuinely effective. Functional aspects were dispersed. Because information operations were part of the information superiority function, they had no direct representation at the table and were not completely integrated into the overarching JTF plans, and thus were not fully leveraged for expertise and use. The after action report noted that senior exercise mentors, the joint task force commander, and the combatant commander all agreed that information operations needed a centralized commander to coordinate activities on the JTF level. A joint information operations task force (JIOTF) would fill this need.

information operations were not completely integrated into the overarching JTF plans

Two concepts are essential in considering information operations on the JTF level. First, combatant commanders must have a strategy in place, clarify the JTF role in achieving the strategy, and accept the strategy as critical to objectives. Second, the role of information operations cannot be simply an afterthought addressed immediately before a conflict. Shaping and influencing activities must occur continuously throughout peace, crisis, and combat. It is almost impossible to change a popular negative view of JTF efforts once shots are fired.

Organization

The need for JIOTF as part of a JTF staff is critical to establish and maintain the knowledge superiority needed to execute rapid decisive operations. Lessons from Allied Force and Enduring Freedom together with observations from Millennium Challenge underscore the need to solve this challenge. Lingering Cold War mentalities still generate operation plans focused on brief, single-dimension combat in which deception, diversion, and feint opportunities are lost. JIOTF should be based on plans and operations. The focus must be on enabling the lethal and nonlethal capabilities of information operations for joint warfighters.

Future experiments should address the need to organize a joint information operations task force to focus on information operations as an element of combat power. The task force would be constituted by members of combatant command staffs, augmented by information operations assets from U.S. Strategic Command as required. The responsibilities of the JIOTF commander would include assisting CJTF planning for information operations, monitoring execution of specific actions, and assessing measures of performance and execution.

Millennium Challenge revealed the important functions that JIOTF brings to the table because the JTF commander recognized information operations as a key element of combat power. The information operations supervisor was a primary staff position with functional responsibilities that included:

- furnishing CJTF with information operations optimized to furnish planning, coordination, integration, and synchronization across the spectrum of conflict
- spanning the CJTF joint operational area with a process harmonized across agencies and services, capable of providing support to other agencies in their missions
- providing a focus for information operations in every medium (land, sea, air, space, and information)
- focusing the command on translating information operations from an enabler into a fully integrated capability
- providing CJTF and component commanders with capabilities, limitations, and employment considerations (second- and third-level effects) to employ information operations.

Millennium Challenge highlighted challenges and areas for future experiments and games. According to the JTF commander, information operations are a "capstone element of combat power . . . both lethal and nonlethal. . . . We must condition the world to accept [information operations] as an essential element." Anyone with responsibility for conducting such operations must have the requisite authority and assets. Because the operations form a component of joint warfighting that remains in a gray area, there is a gap in its effective employment. The challenge is bridging that gap and bringing the full potential of those capabilities to bear against enemies. JFQ